Cassandra Crossing/ Facebook e la privacy del nuovo millennio

(209)— Non basta fare attenzione, non basta configurare tutto con attenzione. Le tecniche e le tattiche degli impiccioni si fanno sempre…

Cassandra Crossing/ Facebook e la privacy del nuovo millennio

Figure 1:

(209)— Non basta fare attenzione, non basta configurare tutto con attenzione. Le tecniche e le tattiche degli impiccioni si fanno sempre più raffinate. Attenti a ciò che cliccate, scattate, pubblicate.

28 gennaio 2011—Vi ricordate di cose si intendeva per "anonimato" e per "difesa della privacy" una ventina di anni fa? Anzi, per far cifra tonda, alla fine del secondo millennio?

Probabilmente no, sia per età relativamente giovane, sia perché i cambiamenti sono stati così grandi e così lenti da renderli difficilmente percepibili.

Persino Cassandra è costretta a fare uno sforzo cosciente per percepirli.

In quei tempi", infatti, una Rete ormai nell'adolescenza era popolata di due tipi di persone: quelli che si sentivano tranquilli, perché in Rete nessuno in effetti aveva interessi ad intercettarli, e quelli che vivevano, a torto od a ragione, investigatori e/o servizi segreti come potenziali impiccioni, e si mettevano tranquilli con un pizzico di crittografia ottenuta via PGP.

Gestione della privacy naturalmente in prima persona: io la difendo, o io la perdo. Oggi non funziona più così. Assolutamente.

In primis oggi la Rete è piena di impiccioni di professione, che per magari legittimi ma anche perversi interessi commerciali e/o di controllo sociale pescano a strascico e sistematicamente i dati del Popolo della Rete.

Inoltre, per la sparuta minoranza che ha qualche interesse a tentare di difendere la propria privacy le cose si sono fatte molto ma molto più difficili, soprattutto per il proliferare dei fattori a cui fare attenzione, alcuni decisamente imprevedibili fino a poco tempo fa.

La disseminazione e l'incrocio dei dati personali la cui fornitura è obbligatoria, come i dati fiscali, quelli del servizio sanitario e quelli censuari è diventato un problema di privacy molto grande, ora che questi dati finiscono sistematicamente in sistemi di data mining e vengono trattati con tecniche di incrocio e deanonimizzazione.

Non è nemmeno il caso di sottolineare che l'Ufficio del Garante per la Protezione dei Dati Personali non abbia ancora nemmeno tentato di affrontare o anche solo stimare questo fenomeno.

Ma il problema di dimensioni maggiori è la perdita indiretta di privacy causata dalle reti sociali come Facebook. Infatti le social network, che ormai stanno evolvendo in social media, incentivano in tutti i modi possibili i loro partecipanti a scambiare quantità sempre maggiori di informazione.

Nuove applicazioni come le liste di preferenze, il tagging di foto, il geotagging, stabiliscono un ponte fra le informazioni che l'incauto socializzatore decide di devolvere alla comunità sociale e quelle di altre persone esterne alla comunità stessa.Facciamo un esempio: applicazioni come il riconoscimento delle caratteristiche delle foto pubblicate possono avere effetti incredibilmente rilevanti sull'estensione della rete di relazioni interne alla comunità sociale verso l'esterno.

I tag EXIF delle foto sono le informazioni che la vostra macchina fotografica inserisce automaticamente in ogni immagine: si tratta di moltissimi dati, incluso di solito il numero di serie della macchina fotografica (avete spedito la garanzia, vero?) e talvolta anche la posizione al momento dello scatto rilevata via GPS, se presente.

Ma è possibile anche distillare dalla sola immagine il rumore di fondo univoco del sensore, che è diverso in ogni macchina: si tratta in pratica dell'*impronta digitale* della macchina fotografica. Questo rende possibile correlare tra di loro le immagini scattate con la stessa macchina fotografica, e di connettere loro tramite informazioni saltellando allegramente tra tag EXIF della foto, tag della comunità sociale ed associazioni tra immagini grazie a feature univoche come il rumore di fondo del sensore.

Non si tratta della predizione di un possibile futuro: le prime due associazioni sono pratica corrente dei gestori della comunità sociali, la terza è una tecnologia di cui esiste la prova di fattibilità, che potrà essere utilizzata (e forse lo è già) dal primo che la riterrà utile.

Non bisogna sottovalutare mai le capacità delle tecniche di data mining, specie quelle non deterministiche ma su base statistica.Riassumendo: la privacy del II millennio si difendeva lottando direttamente contro gli impiccioni, uno scontro chiaro e diretto.

La privacy nel III millennio è ormai una questione molto più complessa.I cattivi e gli impiccioni sono di più, più ricchi e più potenti. Ma il problema più grave è che non ci si deve difendere solo da loro, ma soprattutto dai tuoi "amici".

Dai tuoi conoscenti.

Dai tuoi apparecchi informatici.

Dai tuoi gadget tecnologici.

Uno scenario molto, molto più complicato. E molto, molto peggiore.

Originally published at punto-informatico.it.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

By Marco A. L. Calamari on June 1, 2023.

Canonical link

Exported from Medium on August 27, 2025.